Notice of Allowability	Application No.	Applicant(s)	
	10/697,654	KOTANI, SEIGO	
	Examiner	Art Unit	
	Aubrey H. Wyszynski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the communication filed on 10/31/03*.

2. ☒ The allowed claim(s) is/are *1-47*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 10/31/03 and 1/11/05
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

KAMBIZ ZAND
PRIMARY EXAMINER

DETAILED ACTION

1. Claims 1-47 are pending.

Allowable Subject Matter

2. Claims 1-47 are allowed.

3. The following is a statement of reasons for the indication of allowable subject matter:

Regarding claims 1 and 12:

Bowman-Amuah, U.S. Patent No. 6,842,906 B1 discloses a safety judgment method for judging safety of an information processing apparatus among the information processing apparatus, a first authentication apparatus and a second authentication apparatus which are connected through a communication network, comprising the steps of:

- receiving biological information by said information processing apparatus (col. 82, lines 55-57);
- authenticating the biological information by judging whether the received biological information is proper or not by said information processing apparatus, said first authentication apparatus, or said second authentication apparatus (col. 83, lines 19-20);
- collecting environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus (fig. 27, #2714);

- transmitting the collected environment information from said information processing apparatus to said first authentication apparatus (fig. 95);

Bowman-Amuah fails to teach:

- transmitting an electronic certificate issued in advance by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus from said information processing apparatus to said first authentication apparatus;
- authenticating the electronic certificate by said first authentication apparatus by decrypting the encrypted information with a public key acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted information is proper;
- authenticating the environment information by said first authentication apparatus by judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and
- judging said information processing apparatus to be safe by said first authentication apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the

environment information, and the step of authenticating an electronic certificate are successful.

Regarding claims 1 and 12:

Durst, Jr. et al., U.S. Patent No. 6,434,561 B1 discloses:

- transmitting an electronic certificate issued in advance by said second authentication apparatus and information encrypted with a secret key issued by said second authentication apparatus from said information processing apparatus to said first authentication apparatus (col. 6, lines 52-58);
- authenticating the electronic certificate by said first authentication apparatus by decrypting the encrypted information with a public key acquired from the transmitted electronic certificate by using a public key acquired from said second authentication apparatus, and judging whether or not the decrypted information is proper (fig. 5B);

Durst, Jr. et al., fails to teach:

- authenticating the environment information by said first authentication apparatus by judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and

- judging said information processing apparatus to be safe by said first authentication apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the environment information, and the step of authenticating an electronic certificate are successful.

4. Independent claims 1 and 12 identify distinctive features of authenticating the environment information by said first authentication apparatus by judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and judging said information processing apparatus to be safe by said first authentication apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the environment information, and the step of authenticating an electronic certificate are successful.

In addition to the distinctive features found in claims 1 and 12, independent claims 3 and 36 identify distinctive features of encrypting the collected environment information with a secret key issued by the second authentication apparatus.

In addition to the distinctive features found in claims 1 and 12, independent claims 5, 18, and 25 identify distinctive features of installing the decrypted software in said information processing apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the

environment information and the step of authenticating the electronic certificate are successful.

In addition to the distinctive features found in claims 1 and 12, independent claim 32 identifies distinctive features judging whether or not the decrypted biological information and environment information are proper; environment information authenticating means for judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; biological information authenticating means for judging whether or not the biological information is proper by comparing the decrypted biological information with pre-stored biological information; and safety judging means for judging said information processing apparatus to be safe when all the authentications performed by said biological information authenticating means, said environment information authenticating means and said electronic certificate authenticating means are successful.

In addition to the distinctive features found in claims 1 and 12, independent claims 36 identifies distinctive features of authenticating the biological information by judging whether or not the decrypted biological information is proper by comparing the decrypted biological information with pre-stored biological information.

In addition to the distinctive features found in claims 1 and 12, independent claim 40 identifies distinctive features of said first authentication apparatus judges that the environment information transmitted by said environment information transmitting

means is proper, said first authentication apparatus judges that the electronic certificate and encrypted information transmitted by said encrypted information transmitting means are proper, and said safety judging means receives information indicating that the information is proper.

In addition to the distinctive features found in claims 1 and 12, independent claim 41 identifies distinctive features of installing means for installing the decrypted software in said information processing apparatus when the authentications performed by said biological information authenticating means and said electronic certificate authenticating means are judged successful, said first authentication apparatus judges that the environment information transmitted by said environment information transmitting means is proper, and said installing means receives information indicating that the information is proper.

In addition to the distinctive features found in claims 1 and 12, independent claim 42 identifies distinctive features of said first authentication apparatus judges that the transmitted environment information is proper, the first authentication apparatus judges that the transmitted electronic certificate and encrypted information are proper, and information indicating that the information is proper is received.

In addition to the distinctive features found in claims 1 and 12, independent claim 43 identifies distinctive features of installing the decrypted software in said information processing apparatus when authentications are judged successful in the operation of authenticating the biological information and the operation of authenticating the electronic certificate, said first authentication apparatus judges that transmitted

environment information is proper, and information indicating that the information is proper is received.

In addition to the distinctive features found in claims 1 and 12, independent claim 44 identifies distinctive features of judging whether or not the received environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information.

In addition to the distinctive features found in claims 1 and 12, independent claim 45 identifies distinctive features of when environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus is received from said information processing apparatus, authenticating the environment information by judging whether or not the received environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information.

In addition to the distinctive features found in claims 1 and 12, independent claim 46 identifies distinctive features of the first authentication apparatus judges that environment information transmitted in the step of transmitting environment information is proper, the first authentication apparatus judges that the electronic certificate and encrypted information transmitted in the step of transmitting the encrypted information

are proper, and information indicating that the information is proper is received from said first authentication apparatus.

In addition to the distinctive features found in claims 1 and 12, independent claim 47 identifies distinctive features of causing the computer to install the decrypted software when authentications performed in the step of authenticating the biological information and the step of authenticating the electronic certificate are judged successful, the first authentication apparatus judges that the environment information transmitted in the step of transmitting environment information is proper, and information indicating that the information is proper is received.

5. The closest prior art, Bowman-Amuah teaches receiving biological information and collecting installed environmental information from the information processing apparatus and transmitting the collected environmental information. Durst, Jr. et al., disclose transmitting an electronic certificate and information encrypted with a key and decrypting the information.

The cited prior art fails to teach the following limitation found in claims 1 and 12: authenticating the environment information by said first authentication apparatus by judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information; and judging said information processing apparatus to be safe by said first authentication apparatus when all the authentications performed in the step of

authenticating the biological information, the step of authenticating the environment information, and the step of authenticating an electronic certificate are successful.

Additionally, the cited prior art fails to teach the following limitation found in claims 3 and 36: encrypting the collected environment information with a secret key issued by the second authentication apparatus.

Additionally, the cited prior art fails to teach the following limitation found in claims 5, 18, and 25: installing the decrypted software in said information processing apparatus when all the authentications performed in the step of authenticating the biological information, the step of authenticating the environment information and the step of authenticating the electronic certificate are successful.

Additionally, the cited prior art fails to teach the following limitation found in claim 32: judging whether or not the decrypted biological information and environment information are proper; environment information authenticating means for judging whether or not the transmitted environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the decrypted environment information; biological information authenticating means for judging whether or not the biological information is proper by comparing the decrypted biological information with pre-stored biological information; and safety judging means for judging said information processing apparatus to be safe when all the authentications performed by said biological information authenticating means, said environment information

authenticating means and said electronic certificate authenticating means are successful.

Additionally, the cited prior art fails to teach the following limitation found in claim 36: authenticating the biological information by judging whether or not the decrypted biological information is proper by comparing the decrypted biological information with pre-stored biological information.

Additionally, the cited prior art fails to teach the following limitation found in claim 40: said first authentication apparatus judges that the environment information transmitted by said environment information transmitting means is proper, said first authentication apparatus judges that the electronic certificate and encrypted information transmitted by said encrypted information transmitting means are proper, and said safety judging means receives information indicating that the information is proper.

Additionally, the cited prior art fails to teach the following limitation found in claim 41: installing means for installing the decrypted software in said information processing apparatus when the authentications performed by said biological information authenticating means and said electronic certificate authenticating means are judged successful, said first authentication apparatus judges that the environment information transmitted by said environment information transmitting means is proper, and said installing means receives information indicating that the information is proper.

Additionally, the cited prior art fails to teach the following limitation found in claim 42: said first authentication apparatus judges that the transmitted environment information is proper, the first authentication apparatus judges that the transmitted

electronic certificate and encrypted information are proper, and information indicating that the information is proper is received.

Additionally, the cited prior art fails to teach the following limitation found in claim 43: installing the decrypted software in said information processing apparatus when authentications are judged successful in the operation of authenticating the biological information and the operation of authenticating the electronic certificate, said first authentication apparatus judges that transmitted environment information is proper, and information indicating that the information is proper is received.

Additionally, the cited prior art fails to teach the following limitation found in claim 44: judging whether or not the received environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information.

Additionally, the cited prior art fails to teach the following limitation found in claim 45: when environment information including information about peripheral equipment connected to said information processing apparatus or about software installed in said information processing apparatus is received from said information processing apparatus, authenticating the environment information by judging whether or not the received environment information is proper with reference to an environment information database, which stores environment conditions classified according to information to be transmitted and received, and the transmitted information.

Additionally, the cited prior art fails to teach the following limitation found in claim 46: the first authentication apparatus judges that environment information transmitted in the step of transmitting environment information is proper, the first authentication apparatus judges that the electronic certificate and encrypted information transmitted in the step of transmitting the encrypted information are proper, and information indicating that the information is proper is received from said first authentication apparatus.

Additionally, the cited prior art fails to teach the following limitation found in claim 47: causing the computer to install the decrypted software when authentications performed in the step of authenticating the biological information and the step of authenticating the electronic certificate are judged successful, the first authentication apparatus judges that the environment information transmitted in the step of transmitting environment information is proper, and information indicating that the information is proper is received.

6. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patent No. 6,289,382 B1 to Bowman-Amuah.

b. U.S. Patent Application Publication No. 2003/0154381 A1 to Ouye et al.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Wyszynski whose telephone number is (571)272-8155. The examiner can normally be reached on Monday - Thursday, and alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 5712723811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KAMBIZ ZAND
PRIMARY EXAMINER

AHW